Analysis of the bug

The `do_remotetmp()` function doesn't check for possible dot-dots and slashes in the login name, so it may create files in arbitrary directories. Moreover, the `do_privtmp()` function tries to create the `secret` file without checking that it doesn't already exist; the random name is also easy to guess.